A Survey Paper on Data Transfer via Multimedia With Steganography Methodologies

B.Thenmozhi (M.E.,)[1], J.Santhosh M.E., (Ph.D.,) [2]

[1](Department of Computer Science, K.S.R.College of Engineering
Email: thenmozhib93@gmail.com)

[2] (Assistant Professor, Department of Computer Science, K.S.R College of Engineering
Email: j.santhoshme@gmail.com)

Received: 24-06-2015, **Revised:** 09-08-2015, **Accepted:** 05-09-2015, **Published online:** 26-11-2015

ABSTRACT

Many types of multimedia can be used to conduct pervasive communication like advertisements, posters, videos on TVs, audios, images etc. In this paper basically focuses on the security system based on the Digital Image processing techniques. We can detect and categorize an image feature using the Image Preprocessing Techniques. This paper explains a way to process a Message can be embedded in such images and extracted by a display-and-imaging fashion using smart phones. After applying basic image preprocessing techniques, the image will be again processed with algorithm for Signal-rich-art-image to extract certain kinds of secret information from the target image and infer the contents of an image. The extracted features data then compared with target data and that features are stored in standard database and can be classified. A message synchronization mechanism is also proposed to guarantee correct message extraction is also proposed.

Keywords - **Information hiding, Image Preprocessing, Edge Detection, Steganography, Signal-rich-art-image, High security.**

1. INTRODUCTION

Steganography is a data hiding technique developed in recent years. It is a process that makes use of human perceptive sense of aural redundancy to digital multimedia, and that embeds the secret data in the public media to transfer digital media carrying confidential data to achieve covert communications. Imperceptibility is an important feature of steganography is called anti-detection performance which includes visual imperceptibility and statistical imperceptibility. The imperceptibility is enhanced by improving the method of selecting an appropriate steganographic carrier and improving the matching relationship between carrier image and secret data. Steganography is different from traditional encryption, which is theoretically based on cryptography to hide communication information by encrypting plaintext, but it is difficult to modified the fact that communication occurred, and cipher text transmission will easily arouse the attacker's fears, and then it could be intercepted, attacked. Steganography complements the deficiency of covering of the encryption. Through transmitting communication information hidden secretly in public media, it covers up the facts of real communication purpose and that communiqué occurred. It is not a competitive relation between steganography and encryption, but they can reinforce each other, to further ensure the security of covert communication. This paper studied image steganography based on encryption, which combines secret data of the traditional encryption and information steganography. It not only makes the secret data transmission invisible and incomprehensible, but makes the steganographic system have a higher anti-detection performance.

2.IMAGE STEGANOGRAPHY COMBINED WITH ENCRYPTION

2.1 DES Encryption

Data Encryption Standard uses a 56-bit key and an additional 8-bit parity bit, resulting in the largest 64-bit packet size. This is an iterative block cipher, using the method known as the Feistel, which will encrypt the text block half. The use of sub-key group, half of which application continuous function, and then the outcome with the other half to "XOR" operator followed by the modification of the two and a half, this process will continue, but in the end a cycle of non-exchange. Data encryption standard uses 16 cycles, using XOR, substitution, replacement, four basic arithmetic shift operations. After the hidden data is encrypted, not only the invisibility of information is increased, but also the statistical characteristics of the information and the correlation between information are changed in the same time, which makes the information become 0-1 bit stream, which is in the probability distribution. In order to verify the individuality of encryption algorithm, download three document of 32768 characters from the Internet, and inspect the 0-1circulation in the document before and after encryption. Before the encryption, the number of 0 and 1 is not balanced because of correlation between characters in the natural content, but after the encryption, binary stream of 0 s and 1 s close to equal probability distribution in the document.

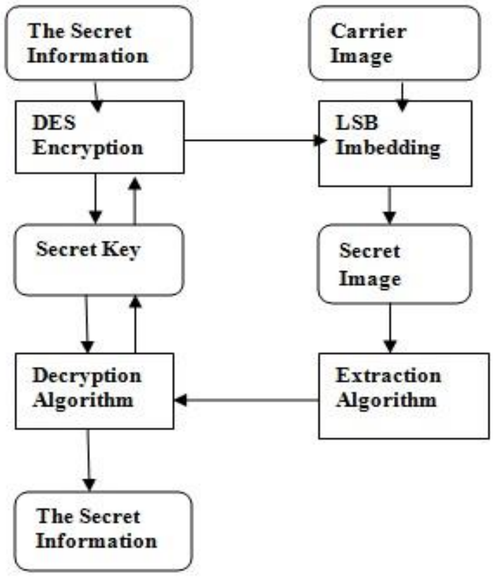
2.2 Digital Image combined LSB Steganography

The LSB (Least Significant Bit) which hides the covert information to the least significant bit of carrier data is the most standard and simplest steganography algorithm, which also features of a high capacity and camouflage. It is still widely measured most practical and applied up to today. The LSB steganography uses the undisclosed data instead of the last bit of the image pixels value, which is correspondent to superimposing a weak indication upon the original carrier signal, and therefore it's difficult to understand visually. But during the embedding process, if the lowest bit of covert data is different from that of pixel rate, we need to change the buck bit of pixel value, namely modify the pixel value 2i to 2i+1 or 2i+1 to 2i. The similarity value convert in the LSB steganography produces parity asymmetry. Fridirich et al. prospect the method of using this unbalanced parity value transforms of LSB to go on RS attack, and Westfield et al. proposed Chi-square test to molest LSB Steganography algorithm. If steganographic process can minimize the deformation of the histogram, it can necessarily resist the attack of analysis methods aforementioned. So in this paper, we propose the steganography collective with encryption, encrypting the information intended to hide before the steganography analysis with encryption preprocessing, and the imperceptibility of the steganography algorithm can be improved by raising the distortion of the histogram.

2.3 Encryption Combined with Image Steganography

In sequence to develop the imperceptibility of Steganography algorithm, this paper studied the Steganography combined with encryption algorithm, which achieve the target by changing the matching relationship between carrier image and secret information. At the transmitting fatal, we firstly select the appropriate image as the carrier, and then encrypt text data or documents designed to hide by DES encryption followed by using the LSB Steganography algorithm to hide the encrypted data in the image; at the getting terminal, firstly extract the encrypted information from the transporter image by the algorithm which is contradictory from Steganography process, and then recover the hidden information by DES decryption algorithm.

Figure2.1. Image Steganography with Encryption



3.SIGNAL RICH ART IMAGE ENCRYPTION AND DECRYPTION

3.1 Pattern Image Creation

Unlike Lee and Tsai's method, which transforms a message into a character message image, the proposed method transforms message into a code Pattern Image similar in appearance to a preselected target image. Specifically, the message is transformed into a bit stream, which is then encoded by binary code patterns in the form of image blocks. Such pattern blocks finally are composed to form the code pattern image. Each pattern block consists of several unit blocks, with each unit block representing a bit of the code pattern of bit stream pattern image. A main issue here is how to design the code patterns so that the corresponding pattern blocks are suitable for use not only in message embedding but in block luminance modulation. To solve this issue, two characteristics must be provided in the designed code patterns: 1) the number Of bits in each code pattern C must be small enough, so that the pattern block representative of C can keep the local color characteristic of the corresponding target image area and 2) the colors of the unit blocks of the pattern block Representative of each code pattern C should not be all the same, because otherwise the original bits represented by the unit blocks of the code patterns will become undistinguishable during the message extraction process.

4. ALGORITHMS

4.1 Canny Edge Detection

The edge recognition process serves to make simpler the analysis of images by drastically reducing the amount of data to be processed, while at the similar time preserving valuable structural information about object boundaries. The Canny edge detector is an edge detection machinist that uses a multi-stage algorithm to detect a wide range of edges in images. It was developed by John F. Canny. Canny too produced a computational theory of edge detection explaining why the technique works.

4.1.1 Smoothing

For the reason that the canny edge detector is susceptible to clatter present in raw unprocessed image data, it uses a filter based on a Gaussian, where the rare image is convolved with a Gaussian filter.

4.1.2 Gradient Calculation

An boundary in an image may point in a diversity of directions, so the Canny Algorithm uses four filters to detect horizontal, vertical and diagonal edges in the blurred image.

5. COMPARISON OF EDGE DETECTION METHODS

It is a very challenging problem to evaluate edge detection results produced by various edge detectors with different parameters. The performance of the edge detector is compared to commonly used or comparable algorithms such as the Canny Sobel and Robert’s boundary detection algorithms. wide-ranging research has been done in creating many different approaches and algorithms for figure segmentation, but it is still complicated to assess whether one algorithm produces more perfect segmentations than another, whether it be for a exacting image or place of images, or more generally, for a whole class of images.

Conventional techniques for perfect detection of edge features, as exemplified by Canny operator, strain such exclusive operations as the iterative use of Gaussians, Laplacians and their designs are largely sequential. Wavelet based boundary detectors provide a ability for varying the scaling factor, which helps in differentiating the weak edges from strong edges. Subjective methods borrowed from the field of psychology and use human judgment to evaluate the performance of edge detectors. On the other hand, objective methods use to measure the performance of edge detectors using signal to noise percentage and mean cube error between the frame detectors images and the original one. Evaluation is complete with both a Receiver Operating Characteristics study and a Chi-square test, and considers the tradeoff between information and disorderliness in the detection consequences. The most excellent edge detector parameter set is then selected by the same arithmetical approach. Results are demonstrated for several edge detection techniques, and compared to published biased evaluation results. Simulation results indicate that the proposed edge detector outperforms competing edge detectors and offers higher performance in boundary detection in digital images corrupted by noise.

5.1 Types of Edges

The usefulness of many image processing and computer visualization tasks depends on the perfection of detecting meaningful edges. Boundary detection has been a demanding problem in low level image processing. It becomes more challenging when paint images are measured because of its multi dimensional scenery. Color images provide accurate information about the entity which will be very practical for further operations than gray scale images. Due to some unavoidable reasons such as deformation, strength variation, noise, segmentation errors, overlap, and occlusion of objects in digital images, it is usually impracticable to take out complete object contours or to segment the whole objects. Due to lack of object edge information the production image is not visually agreeable. A huge number of methods are available in the literature to segment images. This mission is hard and very significant, since the output of an image segmentation algorithm can be fed as contribution to higher-level processing tasks, such as model-based object recognition systems.

6. Joint Feature Learning for Face Verification

In this paper, we recommend an unsupervised attribute learning move toward for face gratitude. Unlike confined face descriptors such as local binary patterns and Gabor features. We propose a aspect learning approach to learn data-adaptive features honestly from underdone pixel standards for face demonstration and detection, so that higher-order data information can be powerfully characterized. While many feature learning methods have been planned in modern years the majority of them learn a single feature hump matrix to convert all patches in images to achieve translation invariance, which is not very important for face recognition applications since there is usually a face position step in a practical face recognition system. For face recognition, dissimilar face regions usually have different structures and it is desirable to learn more region-specific features for face representation. A feasible way to accomplish this goal is to learn feature representations for different face regions independently. However, dissimilar face regions usually share some related information in feature representation and individual feature learning ignores this characteristic. To exploit shared information among different expression regions, we together learn features for unlike face regions, where both the relationship between different face regions and position-specific information are simultaneously exploited for representation. Having obtained features for every regions, we perform spatial pooling for diverse regions to increase their representative capability.

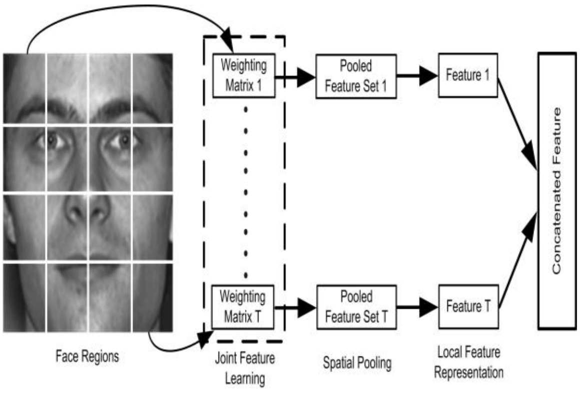


Figure 6.1 Joint Feature Learning For Face Feature Detection

FUTURE WORK

A lot of types of identities presented in the human surroundings can be used as signal-rich-art carriers, such as digital media, pictorial material, art work, and so on. In recording human visual observation results, the video distinctiveness has more imaginative effects than other types of identities. In this paper, we define signal-rich-art image as the type of signal-rich art with its identity being an video which can be not only any digital file, but also any real object, such as posters, labels, illustrations. Signal-rich-art images can help people to perform Ubiquitous computing; they can substitute information via such images existing in the environment everywhere and anytime.

CONCLUSION

This paper mainly focus on the steganography carried by image, which combines Data Encryption Standard (DES) encryption with LSB algorithm and equipment twin protect of unseen data, making the secret information 31258 incomprehensible and undetectable. In addition, the DES encryption algorithm changes the algebraic individuality of the secret data, and improves the lowest identical degree of its bit stream and transporter image, leading to a better imperceptibility of steganographic algorithm. Also another kind of technique is proposed, that is Signal Rich Art Image Encryption and Decryption with secret key. Skillful techniques of code pattern blueprint, unit block segmentation, pattern block classification, and so on, have been proposed for message data embedding and taking out. Signal-rich art code image has several qualities: 1) the image has the visual exterior of any preselected target representation 2) the proposed system can tolerate more distortions in acquired versions of the code image like perspective transformation, noise, screen blurring 3) The secret message can be extracted from an image captured by a mobile device. The main goal is to propose appropriate data hiding techniques to create various type of message-rich multimedia for pervasive communication. Fulfillment of this goal will be expected to enhance the state-of-art studies on data hiding techniques, yielding new visions of pervasive Communication and further steps of extending its applications.

REFERENCES

[1] Roszizti Ibrahim Teoh Suk Kuan.Steganography Aglorithm to Hide Secret Message inside an Image[J]. Technology and Application of Compute: English, 2011,2(2),102-108

[2] Der-Chyuna Lou, Chen-Hao Hu, LSB steganogrpahic method based on reversible histogram transformation function for resisting statistical steganalysis[J], Information Sciences,2012, 188:346-358.

[3] Yifeng Sun,Fenlin Liu, Selecting cover for image steganography by correlation coefficient [C] ,2010 Second International Workshop on Educaton Technology and Computer Science, 159-162.

[4] Marwaha, P., Visual cryptographic steganogrpahy in images[C], Computer Communication and Networking
Technologies (ICCCNT), 2010 International Conference 2010:1-6.

[5] Fridrich J, Goljan M, Du R, Detecting lsb steganography in color and gray-images[C],IEEE Multimedia Special Issue on Security, 2001:22-23.

[6] A.Westfeld, A, Pfitzmann, Attacks on steganographyic system, Proceedings of the 3rd International Workshop on Information Hiding, Dresden, Germany, 1999:61-76

[7] Ya-Lin Lee and Wen-Hsiang Tsai, A New Data Transfer Method via Signal- Rich-Art Code Images
Captured by Mobile Devices, IEEE Transaction on Circuits and Systems for Video Technology, April. 2015.

[8] Shijie Li and Dapeng Oliver Wu, “Modularity-Based Image Segmentation”, IEEE Transaction on image processing, April. 2015.